Print this page

Mozilla - CA Program

Case Information

Case Number	00000022	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	IdenTrust	**Request Status**	Pending Approval

Additional Case Information

Subject	Included renewed roots	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1037590

General information about CA's associated organization

Company Website	http://www.identrust.com/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	USA	**Verified?**	Verified
Primary Market / Customer Base	IdenTrust is a for-profit corporation serving the private, commercial, and government sectors.	**Verified?**	Verified
Impact to Mozilla Users	Renew root certificates that were included via Bug #394733. The original roots are in all the major browsers.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	TrustID CPS: 3.2.7.1 Verification against High Risk and Denied Request Lists ACES CPS Addendum: Section 3.1.9.4 – Authentication of Component Identity TrustID CPS: 4.9 CERTIFICATE REVOCATION AND SUSPENSION ACES CPS: 4.4 CERTIFICATE REVOCATION	**Verified?**	Verified

DNS names are included in the SAN extension. The name included in the CN is replicated in the SAN.

IdenTrust issues SSL certificates only to organizations. The existence of the organization is validated. For Commercial root see TrustID CPS section 3.2, the table that establishes what is validated and sections 3.2.2 and 3.2.2.1, and ACES CPS Addendum 3.1.8.

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	Currently, IdenTrust does not issue Domain Validated certificates. If, in the future, DV certificates are issued, they will comply with current policy that limits certificates to 39 months. Wildcard SSL Certificates for the commercial root are OV. TrustID CPS section 3.1.2: The entire Domain Namespace in Wildcard Certificates must be rightfully controlled by the Subscriber Organization. IdenTrust validates Domains for SSL certificates issued and does not delegate such validation. See TrustID CPS section 3.2.7.2 and ACES CPS Addendum 3.1.9.4. IdenTrust allows Trusted Agents to, in particular cases, manually validate the email of certificates. Trusted Agents are employees of the organizations requesting the certificate and are under agreement with IdenTrust. Trusted Agents validation is limited to emails within their organization and only in circumstances where automatic validation is not possible. See TrustID CPS section 3.2.5 and ACES CPS Addendum section 3.1.9.7 for detail. Commercial Root CA: There is a possibility of externally operated subordinate CAs. In such case, IdenTrust will favor the externally audited and publicly disclose model of operation. TrustID CPS: 3.2.7.3 Verification of DBA or Tradename: "…IdenTrust does not and will not issue SSL Certificates to reserved IP addresses or internal server names. " ACES CPS Addendum: 1.3.2.3.1 – Agency and Relying Party Application SSL Server Certificates: "…IdenTrust does not and will not issue SSL Certificates to reserved IP addresses or internal server names. "	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Case No	R00000026	**Case Number**	00000022
Request Status	Pending Approval	**Root Certificate Name**	IdenTrust Commercial Root CA 1

Additional Root Case Information

Subject	Include IdenTrust Commercial Root CA 1

Technical Information about Root Certificate

O From Issuer Field	IdenTrust	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This SHA-256 root will eventually replace the SHA-1 “DST Root X3” certificate that was included via Bug #394733. The intent is to issue email and SSL certificates.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org /attachment.cgi?id=8473319	**Verified?**	Verified
Valid From	2014 Jan 16	**Verified?**	Verified
Valid To	2034 Jan 16	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://sha2ssl-trustidvalid.identrustssl.com/	**Verified?**	Verified
CRL URL(s)	http://validation.identrust.com /crl/commercialrootca1.crl http://validation.identrust.com /crl/trustidcaa52.crl (CRL NextUpdate: 24 hours) TrustID CPS section 4.9.7: twenty-four hours	**Verified?**	Verified
OCSP URL(s)	http://commercial.ocsp.identrust.com	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested	Not Requesting EV Treatment at this time	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	DF:71:7E:AA:4A:D9:4E:C9:55:84:99:60:2D:48:DE:5F:BC:F0:3A:25	**Verified?**	Verified
SHA-256 Fingerprint	5D:56:49:9B:E4:D2:E0:8B:CF:CA:D0:8A:3E:38:72:3D:50:50:3B:DE:70:69:48:E4:2F:55:60:30:19:E5:28:AE	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The intent is to generate the subordinate CA Certificates that will support our current lines of business under the root being replaced. At this time not all of the subordinate CA certificates have been generated (names may change) - [Internal]TrustID CA A52 (s/mime certificates) - [Internal]TrustID CA A12 (Device/SSL Certificates)	**Verified?**	Verified
Externally Operated SubCAs	Currently none. In the future, there is the possibility of issuance of externally operated CAs under this root. In such case, IdenTrust will favor the independently audited and publicly disclose subordinate CA model of operation. Note that the “DST Root X3” root has signed one subordinate CA that is externally operated. This subordinate CA has a policy publicly published and has been audited under the WebTrust regime.	**Verified?**	Verified
Cross Signing	This root is not cross-certified	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Under the “DST Root X3” root there are external RAs who can issue certificates. Those RAs are bound by legal agreement to follow the Trust ID CP/CPS in issuing certificates. IdenTrust does not currently have RAs who can approve SSL certificates. For the issuance of SSL certificates within large organizations, IdenTrust uses the Enterprise RA role in consistency with Baseline Requirements. For this use case, IdenTrust has implemented procedural and technical controls. In this instance, IdenTrust LRAs verify the domain ownership/control in every case (See TrustID CPS section 3.2.7.2). Then, systems are configured to allow the issuance of SSL certificates that are derivative subdomains of those domains previously authorized. Enterprise RAs have a limited role. TrustID Section 5.2.4.12 outlines their functions. Only LRAs that work for IdenTrust or an RA can verify domain ownership/control of a domain name.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English.	**Verified?**	Verified
CA Document Repository	https://secure.identrust.com/certificates/policy/ts/	**Verified?**	Verified
CP Doc Language	English		
CP	https://secure.identrust.com/certificates/policy/ts/TrustID_CP_v1.6.1_20130912.pdf	**Verified?**	Verified
CP Doc Language	English		

CPS	https://secure.identrust.com/certificates/policy/ts/identrust_trustid_cps_v2.3_20140109.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	BrightLine	**Verified?**	Verified
Auditor Website	https://www.brightline.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1720&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	7/25/2014	**Verified?**	Verified
BR Audit	https://secure.identrust.com/certificates/policy/ts/current-baseline-requirements-audit.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	9/19/2014	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	TrustID CP section 3.1.8	**Verified?**	Verified
SSL Verification Procedures	TrustID CPS section 3.2.7.2: IdenTrust verifies that the PKI Sponsor has the right to use or has control of the FQDN(s) or IP address(es) listed in the Certificate application by following the steps listed below. The LRA confirms the Domain registrant's rights by doing the following: 1) The Domain(s) supplied by the PKI Sponsor is placed into a search engine (e.g. WHOIS) and the LRA records the contact information for the Domain Name Registrant. 2) Once the Domain Name registrant is identified from a database record he or she is contacted via email. In this email the Domain Name registrant will be asked: a. to confirm or deny the right of the PKI Sponsor to be issued a Device Certificate for the Domain Name(s) for which the PKI Sponsor has applied; b. if they would like to provide the names other potential PKI Sponsor(s) that may request the same type of Certificate; and c. with respect only to applications for Wildcard Certificates, to confirm or deny control over the entire Domain Namespace of the FQDN provided and that such control is rightful. If the PKI Sponsor applies for a Domain Name that contains a two-letter country	**Verified?**	Verified

	code (ccTLD) (e.g. www.identrust.uk as opposed to www.identrust.com), this confirmation will be sought from the Domain Name level to which the ccTLD applies. This means that the LRA cannot obtain verification from www.identrust.com if the PKI Sponsor is applying for a Domain Name from www.identrust.uk.		
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	Trust ID CPS section 3.2.2.1, Verification of Sponsoring Organization Legal Existence TrustID CPS section 3.2.2.2, Authentication of the Individual-Organization Affiliation	**Verified?**	Verified
Email Address Verification Procedures	Trust ID CPS section 3.2.5: Email verification when required can be done in two ways; electronically and manually through a list submitted by a Trusted Agent. If the application for a Certificate requires email verification the application cannot be approved until the specified steps for electronic or manual verification is complete. - Electronic: When an Applicant/PKI Sponsor submits an application through a secure online form, an automated email is sent to the personal email address provided in the application. Within that automated email message there is a link that guides the Applicant/PKI Sponsor to a server-authenticated SSL/TLS secured web site and instructions to provide out-of-band information, including an Account Password. This Account Password was created during the application by the Applicant/PKI Sponsor and it is secure only to the Applicant/PKI Sponsor. When the Applicant/PKI Sponsor provides and submits the Account Password created during the application accurately the verification of the email address is completed and the verification status is automatically updated within the Applicant/PKI Sponsor's application record. - Manual: When a Trusted Agent provides the list of authorized Applicants/PKI Sponsors, the email address is validated by the Trusted Agent based on the internal knowledge of the Sponsoring Organization. The Trusted Agent may use internal databases and directories to ensure the email accuracy.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	Two-factor authentication based on digital-certificate-based access and access control lists (ACLs) are used to access the system capable of issuing a certificate. For humans approving certificates: Hardware tokens; FIPS 140-1/2 Level 2-validated hardware.	**Verified?**	Verified

	For automated RA: Hardware or software cryptomodules All RAs are required to use digital certificates and be in the ACL.		
Network Security	TrustID CPS sections 5.7.1, 6.6.2, 6.7, and 8	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://testssl.identrust.com/	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Case No	R00000027	**Case Number**	00000022
Request Status	Pending Approval	**Root Certificate Name**	IdenTrust Public Sector Root CA 1

Additional Root Case Information

Subject	Include IdenTrust Public Sector Root CA 1

Technical Information about Root Certificate

O From Issuer Field	IdenTrust	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This SHA-256 root will eventually replace the SHA-1 “DST ACES X6” certificate that was included via Bug #394733. The intent is to issue email and SSL certificates.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8473320	**Verified?**	Verified
Valid From	2014 Jan 16	**Verified?**	Verified
Valid To	2034 Jan 16	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://sha2ssl-acesvalid.identrust.com/	**Verified?**	Verified
CRL URL(s)	http://validation.identrust.com/crl/publicrootca1.crl http://validation.identrust.com/crl/acesca2.crl (CRL NextUpdate: 24 hours) ACES CPS section 4.4.5.1: 18 to 24	**Verified?**	Verified

	hours		
OCSP URL(s)	http://public.ocsp.identrust.com	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested	Not requesting EV treatment at this time.	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	BA:29:41:60:77:98:3F:F4:F3:EF:F2:31:05:3B:2E:EA:6D:4D:45:FD	**Verified?**	Verified
SHA-256 Fingerprint	30:D0:89:5A:9A:44:8A:26:20:91:63:55:22:D1:F5:20:10:B5:86:7A:CA:E1:2C:78:EF:95:8F:D4:F4:38:9F:2F	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	At the time of generation of this document, the intent is to generate the following subordinate under this root: - [Internal]IdenTrust ACES CA 2 (s/mime, device/SSL certificates)	**Verified?**	Verified
Externally Operated SubCAs	There are no plans to have externally operated subordinate CAs off this root at this time Note that there are no externally-operated subordinate CAs that have been signed by the “DST ACES X6” root.	**Verified?**	Verified
Cross Signing	This root is not cross-certified	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	There are currently no third-party issuers for this root. There are currently no third-party issuers (e.g. RAs) that can cause the issuance of certs in the CA hierarchy of the “DST ACES X6” root. IdenTrust validates Domains for SSL certificates issued and does not delegate such validation. See ACES CPS Addendum 3.1.9.4. Comment #8: Only LRAs that work for IdenTrust or an RA can verify domain ownership/control of a domain name. LRAs are obligated to follow the procedures outlined in the CPS. Currently, IdenTrust does not have any RAs that approve SSL certificates under this policy and root. ACES CPS Addendum Section 3.1.9.4 explains the	**Verified?**	Verified

	practices around domain ownership/control validation. Under this CP/CPS, the Enterprise role does not currently exist.		

Verification Policies and Practices

Policy Documentation	ACES Documents are in English	**Verified?**	Verified
CA Document Repository	https://secure.identrust.com/certificates/policy/aces/	**Verified?**	Verified
CP Doc Language	English		
CP	https://secure.identrust.com/certificates/policy/aces/	**Verified?**	Verified
CP Doc Language	English		
CPS	https://secure.identrust.com/certificates/policy/aces/dst-aces-cps-v20040617.pdf	**Verified?**	Verified
Other Relevant Documents	ACES CPS Addendum: https://secure.identrust.com/certificates/policy/aces/IdenTrust-Addendum-2013-11-26.pdf	**Verified?**	Verified
Auditor Name	BrightLine	**Verified?**	Verified
Auditor Website	https://www.brightline.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1720&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	7/25/2014	**Verified?**	Verified
BR Audit	https://secure.identrust.com/certificates/policy/ts/current-baseline-requirements-audit.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	9/19/2014	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	ACES CPS Addendum section 1.1	**Verified?**	Verified
SSL Verification Procedures	ACES CPS Addendum section 3.1.9.4: Verification of Authorization by Domain Name Registrant IdenTrust verifies that the PKI Sponsor has the right to issue or has control of the Fully-Qualified Domain Name(s) from the SAN extension and public IP address(es) listed in the Certificate application by following the steps listed below.	**Verified?**	Verified

	The LRA confirms the rights by the Domain Registrant by doing the following: (1)The domain(s) supplied by the PKI Sponsor is placed into a search engine (e.g. WHOIS) and the LRA records the contact information for the Domain Name Registrant. (2) Once the Domain Name Registrant is identified from a database record he or she are contacted via email to confirm the information provided by the PKI Sponsor to confirm or deny the right of the PKI Sponsor to be issued the certificate for the Domain Name(s) for which the PKI Sponsor has applied. It is through this process that IdenTrust ensures that SSL Certificates are issued with the consent of the owner of each FQDN contained within the Certificate.During this exchange the Domain Name Registrant will have the opportunity to name other potential PKI Sponsor(s). If the PKI Sponsor applies for a domain that is a two-letter country code (ccTLD), this confirmation will be sought from the Domain Name level to which the ccTLD applies.		
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	ACES CPS Addendum section 3.1.8: Authentication of Sponsoring Organization Identity	**Verified?**	Verified
Email Address Verification Procedures	ACES Addendum section 3.1.9.7 Email verification when required can be done in two ways; electronically and manually through a list submitted by a Trusted Agent. If the application for a Certificate requires email verification the application cannot be approved until the specified steps for electronic or manual of verification is complete. Electronic: When an Applicant/PKI Sponsor submits an application through a secure online form, an automated email is sent to the Applicant/PKI Sponsor's email address provided in the application. Within that automated email message there is a link that guides the Applicant/PKI Sponsor to a server-authenticated SSL/TLS secured web site and instructions to provide out-of-band information, including in Account passphrase Password. This Account Password was created during the application by the Applicant/PKI Sponsor and it is secure only to the Applicant/PKI Sponsor. When the Applicant/PKI Sponsor provides and submits the passphrase Account Password created during the application accurately the verification of the email address is completed and the verification status is automatically updated within the Applicant/PKI Sponsor's application	**Verified?**	Verified

	record. Manual: When a Trusted Agent provides the list of authorized Applicants/PKI Sponsors, the email address is validated by the Trusted Agent based on the internal knowledge of the Sponsoring Organization. The Trusted Agent may use internal databases and directories to ensure the email accuracy.		
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit.	**Verified?**	Verified
Multi-Factor Authentication	Two-factor authentication based on digital-certificate-based access and access control lists (ACLs) are used to access the system capable of issuing a certificate. For humans approving certificates: Hardware tokens; FIPS 140-1/2 Level 2-validated hardware. For automated RA: Hardware or software cryptomodules All RAs are required to use digital certificates and be in the ACL.	**Verified?**	Verified
Network Security	ACES CPS sections 5.7.1, 6.5.1.1, and 6.7.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://testssl.identrust.com/	**Verified?**	Verified